Virginia Department of Health
Division of Child and Adolescent Health

Information Systems: Security and Confidentiality Policies, Procedures, and Standards

For

- VDH Employees
- CCC-SUN, VISITS, and LEADTRAX
  - Contractors
  - Data Users
  - Data Recipients

Created: June 10, 2002
Revised: May 29, 2003
Revised: February 3, 2004

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment

division of child And Adolescent health

Virginia Department of Health
Division of Child and Adolescent Health

Information Systems:
Security and Confidentiality Policies, Procedures, and Standards [1,2]

CERTIFICATE OF RECEIPT

Your signature below indicates your receipt of this document, which is entitled *Information Systems: Security and Confidentiality Policies, Procedures, and Standards: For VDH Employees, CCC-SUN / VISITS/LeadTrax Contractors, CCC-SUN / VISITS/LeadTrax Data Users, and CCC-SUN / VISITS/LeadTrax Data Recipients,* Virginia Department of Health, Division of Child and Adolescent Health, revised **February 3, 2004**. Your signature also indicates that you have read and have had an opportunity to ask questions and obtain responses in order for you to understand the content of the document.

Your signature does not imply agreement or disagreement with the standards; however, all contractors and/or data recipients are required to comply with *Information Systems: Security and Confidentiality Policies, Procedures, and Standards: For VDH Employees, CCC-SUN / VISITS/LeadTrax Contractors, CCC-SUN / VISITS/LeadTrax Data Users, and CCC-SUN / VISITS/LeadTrax Data Recipients,* Virginia Department of Health, Division of Child and Adolescent Health, which was **created June 10, 2003, revised May 29, 2003, and revised February 3, 2004**.

Legal Name *(print)*: ______________________________
Signature: ______________________________ Date: _______
Organization: ______________________________

Revised **02/03/04**

CC: Contractor/data recipient
Program File

[1] Information Systems Audit Item 11: Provide evidence that the Information Security Policies & Procedures have been developed for this application by the project management.

[2] Information Systems Audit Item 20: Provide evidence that the Information Security Policies & Procedures have been Distributed to End-User by the Organization, e.g. posted on the VDH Internal Web Page is considered distributed.

TABLE OF CONTENTS

PREFACE

DCAH. The Division of Child and Adolescent Health (DCAH) is located in Richmond, Virginia, and along with four other divisions and one center, provides the framework for the Virginia Department of Health (VDH) Office of Family Health Services.

DCAH Mission. The mission of DCAH is to promote the health of children and adolescents in Virginia. The vision is that "we are leaders in assuring that children and adolescents reach their full physical, emotional, social, and intellectual health potential."

DCAH Information Systems: Confidentiality and Security Policies, Procedures, and Standards. The collection, entry and analysis of DCAH data are principle functions used to shape DCAH surveillance and prevention activities. The following documentation serves as the official policies, procedures, and standards for DCAH confidentiality and security pertaining to all DCAH data. This includes the information systems CCC-SUN, VISITS, and LeadTrax, which are hosted and supported by Welligent, LLC—a subsidiary of the Children's Health System. These standards are also posted by Welligent on each application's message center as a document that can be downloaded. Due to the importance and sensitive nature of DCAH confidential documentation, a variety of security issues are repeated throughout these standards.

CCC-SUN / VISITS/LeadTrax Information Systems Contractors, Data Users, Data Recipients. Certain text within this document is more applicable to DCAH staffs, as opposed to DCAH information systems and service contractors, data users, and data recipients. This information has been intentionally included in this document to serve as examples of DCAH policies, practices, and standards.

> Note. *DCAH information systems and service contractors, data users, and data recipients should ensure that their security standards are at least equivalent to the standards described in this document.*

Available Online. This document will soon be available online at the following DCAH web page: www.vahealth.org/childadolescenthealth/pubsdcah.htm.[3]

Approved: Joanne S. Boise (Signature on file)
Director, Division of Child and Adolescent Health
Overall Responsible Party (ORP) for Division Security and Confidentiality[4],

Effective Date: June 10, 2002

[3] Information Systems Audit Item 20: Provide evidence that the Information Security Policies & Procedures have been Distributed to End-User by the Organization, e.g. posted on the VDH Internal Web Page is considered distributed

[4] Information Systems Audit Item 11: Provide evidence that the Information Security Policies & Procedures have been developed for this application by the project management

SECTION 1. DOCUMENTATION

Best Security Practices [5]

Project Managers and Vendors. Project Managers and vendors—DCAH's primary information systems developer and information systems management contractor[6]—are provided and familiar with the following best security practices, which are requirements for the management of secure information

- Federal information systems security laws, policies, standards, directives, regulations, and guidelines.
- State information systems security laws, policies, standards, directives, and guidelines.
- VDH information systems security laws, policies, standards, directives, and guidelines.
- HIPAA proposed IT security regulations.

Welligent. DCAH's primary information systems developer and information systems management contractor for CCC-SUN, VISITS, and LeadTrax information systems is Welligent, Limited Liability Company (LLC), a subsidiary of the Children's Health System. (Welligent, LLC was formerly known as Health Informatics.)

State and Federal Laws and Regulations [7]

Relevant sections of the *Code of Virginia* and federal Social Security Act and the Commonwealth of Virginia regulations pertaining to the information systems in DCAH are listed below.

Care Connection for Children System Users Network (CCC-SUN)

Confidentiality. *Code of Virginia*, §§ 2.1-342, 2.1-377-386, 32.1-127.1:03 and 32.1-127.1:04.

Reporting Requirements. *Code of Virginia* §§ 32.1-14, 32.1-77, 32.1-78 and Sections 505 and 506 of the federal Title V Social Security Act.

Security Standards. VDHITRM Policies and Procedures, COV ITRM Standard SEC2001-01.1 and Proposed Security and Electronic Signature Standards, (HCFA-0049-P) for the federal Health Insurance Portability and Accountability Act of 1996.

[5] Information System Audit Item 9: Provide evidence that the data security requirements (Federal and State Laws, Regulations, etc.) have been identified and documented.

[6] CCC-SUN / VISITS Vendor is Welligent, LLC, 905 Redgate Avenue, Suite 102, Norfolk, Virginia 23507.

[7] Information System Audit Item 9: Provide evidence that the data security requirements (Federal and State Laws, Regulations, etc.) have been identified and documented.

Virginia Infant Screening and Infant Tracking System (VISITS)-Hearing Module

Confidentiality. *Code of Virginia* §§ 2.1-342, 2.1-377-386, 32.1-64.2, 32.1-127.1:03 and 32.1-127.1:04.

Reporting and Screening Requirements. *Code of Virginia* §§ 32.1-64.1 and 12 VAC 5-80 and Sections 505 and 506 of the federal Title V Social Security Act.

Regulations. *Regulations for Administration of the Virginia Hearing Impairment Identification and Monitoring System,* 12 VAC5-80.

Security Standards. VDHITRM Policies and Procedures, COV ITRM Standard SEC2001-01.1 and Proposed Security and Electronic Signature Standards, (HCFA-0049-P) for the federal Health Insurance Portability and Accountability Act of 1996.

Virginia Infant Screening and Infant Tracking System (VISITS)-VaCARES Module

Confidentiality. *Code of Virginia* §§ 2.1-342, 2.1-377-386, 32.1-69.2, 32.1-127.1:03 and 32.1-127.1:04.

Reporting and Education Requirements. *Code of Virginia* §§ 32.1-69.1, 32.1-69.1:1 and Sections 505 and 506 of the federal Title V Social Security Act.

Security Standards. VDHITRM Policies and Procedures, COV ITRM Standard SEC2001-01.1 and Proposed Security and Electronic Signature Standards, (HCFA-0049-P) for the federal Health Insurance Portability and Accountability Act of 1996.

Virginia Infant Screening and Infant Tracking System (VISITS)-Metabolic Module

Confidentiality. *Code of Virginia* §§ 2.1-342, 2.1-377-386, 32.1-67.1, 32.1-69, 32.1-127.1:03 and 32.1-127.1:04.

Regulations. *Rules and Regulations of the Board of Health, Commonwealth of Virginia, Governing the Newborn Screening and Treatment Program* VR 355-11-200, July 14, 1993.

Reporting, Screening, and Treating Requirements. *Code of Virginia* §§ 32/1-65, 32.1-66, 32.1-67, 32.1-68 and Sections 505 and 506 of the federal Title V Social Security Act.

Security Standards. VDHITRM Policies and Procedures, COV ITRM Standard SEC2001-01.1 and Proposed Security and Electronic Signature Standards, (HCFA-0049-P) for the federal Health Insurance Portability and Accountability Act of 1996.

Childhood Lead Poisoning Prevention Program (CLPPP) Database-LeadTrax

Confidentiality. *Code of Virginia*, *Virginia* §§ 2.1-342, 2.1-377-386, 32.1-67.1, 32.1-69, 32.1-127.1:03 and 32.1-127.1:04.

Regulations. *Regulations for Testing Children for Elevated Blood Lead Levels.* 12 VAC 5-120-10 through 12 VAC 5-120-90.

Reporting Requirements. Required by the *Regulations for Disease Reporting and Control,* Commonwealth of Virginia, State Board of Health, January 1999, pages 8-10. *Code of Virginia* § 32.1-36, 12 VAC 5-90-80, 12 VAC 5-90-90, 12 VAC 5-120-70, 12 VAC 5-120-70 Samples submitted to a qualified laboratory.

Security Standards. Virginia Department of Health Information Technology Resource Manual Policies and Procedures, Code of Virginia Information Technology Resource Manual Standard SEC2001-01.1 and Proposed Security and Electronic Signature Standards, (HCFA-0049-P) for the Federal Health Insurance Portability and Accountability Act of 1996.

DCAH Documentation

Responsible Parties

Overall Responsible Party (ORP). The Director of the Division of Child and Adolescent Health serves as the Overall Responsible Party (ORP) for all DCAH security and confidentiality issues, including—with assistance from DCAH supervisors—monitoring and ensuring the day-to-day security of DCAH data and associated paperwork.

Project Managers. The Project Manager for the information system is responsible for chairing the application's security committee, coordinating the continuous collection and provision of evidence to an information systems auditor during the information systems security audit consultation phase, requesting an audit review by the internal auditor, and giving status on the *Information Systems Security Audit Check List* tasks during the audit review.

Program Managers and Vendors. As assigned by the Project Manager, program managers and vendor[8]— DCAH's primary information systems developer and information systems management contractor— provide evidence to an information systems auditor during the information systems security audit consultation phase and give status on *Information Systems Security Audit Check List* tasks during the audit review.

Contractors, Data Users, Data Recipients. DCAH requires signed documentation, utilizing the enclosed Certificate of Receipt for new contractors, data users, and data recipients, and renewed signatures on an annual basis for existing contractors/data

[8] CCC-SUN / VISITS Vendor is Welligent, LLC, 905 Redgate Avenue, Suite 102, Norfolk, Virginia 23507.

recipients, for the purpose of ensuring relevant personnel are initially informed and remain familiar with DCAH policy pertaining to the security and confidentiality of sensitive data. The text of this document addresses issues such as confidentiality, and information systems security/access. The original signed copy of the Certificate of Receipt by employees and contractors is kept on file at OFHS Business Section. All other certificates are kept on file at DCAH. Signed copies are returned to the contractor/data recipient for their official records.

Each DCAH contractor, data user, and data recipient receives a copy of these standards for their files. All DCAH policies and procedures, including the Security and Confidentiality Standards, are distributed to DCAH and pertinent local health department staff.

Information Systems Security Officer (ISSO) [9]

Host Information Systems Security Officer (Host ISSO) Duties

DCAH's primary information systems developer and information systems management contractor for CCC-SUN, VISITS, and LeadTrax information systems is Welligent, LLC. CCC- SUN, VISITS, and LeadTrax reside on a server that is hosted by Welligent, LLC. As part of their contractual agreement with VDH, Welligent, LLC performs the Host ISSO tasks.

Tasks. The Host ISSO is responsible for performing all of the following tasks.

1. Add privileges to accounts based on user management instructions and a written approval process.
2. Establish accounts at user management direction based upon a written approval process.
3. Manage access control and create user accounts and temporary passwords.
4. Monitor, audit, test systems and networks for possible security problems.
5. Review security logs files on a daily basis and investigate anomalies as needed. A list of these logs and investigated anomalies is to be sent to the Agency ISSO once a week.
6. Test, install, and maintain security infrastructure tools.
7. Perform periodic war dialing to check for unauthorized modems.
8. Test and install patches and fixes for security vulnerabilities in Welligent, LLC, software.
9. Periodically run a password-cracking tool to ensure passwords meet the minimum strength requirements established in the organization security policy. Establish minimum default parameters for user passwords.
10. Perform regular automated system check to reveal possible intruder activity or illicit activity by insiders.
11. Perform random security audits to test for conformance to security policies and standards, or to check for the existence of a specific class of problems.

[9] Information System Audit Item 10: Provide evidence of the written assignment of information systems security responsibilities, e.g. .job description and job expectations for site security officer, agency system security officer.

12. Audit critical files (e.g./etc/password) and router configurations nightly to assess their integrity and to look for unauthorized changes.
13. Audit user account activity on a regular basis to detect dormant, invalid, or misused accounts. The Agency ISSO will review this activity periodically. A list of these logs and investigated anomalies is to be sent to the Agency ISSO at least monthly.

Agency Information Systems Security Officer (Agency ISSO) Duties

The VDH Systems Security Officer performs the Agency ISSO tasks for CCC-SUN, VISITS, and LeadTrax. As for all other divisions within VDH, the Systems Security Officer for VDH assists DCAH in the development and maintenance of security standards. The VDH Systems Security Officer is a member of the Security Committees for CCC-SUN, VISITS, and LeadTrax. The Project Managers for CCC-SUN, VISITS, and LeadTrax collaborate with the Agency ISSO and the VDH Systems Security Officer to obtain changes in security standards, to incorporate the changes in the DCAH document, and to ensure adherence to security standards by Welligent, LLC and data users and recipients.

Tasks. The Agency ISSO is responsible for performing all of the following tasks.

1. Help recommend and develop internal security standards.
2. Help define, produce, and maintain official security policy and documentation.
3. Monitor security newsgroups, mailing lists, and posting and respond to them accordingly (e.g. install necessary security patches).
4. Stay current on security technology and possible threats to the organization.
5. Provide investigation, coordination, reporting, and follow-up of network security incidents.
6. Participate in reviews and analysis of internal projects that may have an impact on the security of the organization.
7. Advocate corporate information security policy and procedures to internal and external clients, customers, users, and staff.
8. Provide security awareness training to management, information technology support staff, users, and raise security consciousness at all levels of the organization.
9. Audit new system installations or system modifications to ensure conformance to existing policies and standard system configuration.
10. Perform periodic audits and vulnerability assessments to determine the overall state of security.
11. Help the organization balance resources expended against the most likely areas of weaknesses.
12. Review periodically the signed Information System Security Access Agreements for the created user accounts.

Certificate of Receipt

The Certificate of Receipt serves as the official DCAH documentation pertaining to knowledge of *Information Systems Security and Confidentiality Policies, Procedures, and Standards: For DCAH Information Systems Employees, Contractors, Data Users, and Data Recipients*, Virginia Department of Health, Division of Child and Adolescent

Health. This certificate shall suffice as the only DCAH-specific documentation requiring signature. It shall be updated annually.

Statement of Confidentiality

All persons working in DCAH are required to maintain and protect confidential records and related documents. To ensure that all personnel, on-site contractors and data recipients understand and are aware of the responsibilities of maintaining confidentiality, all are provided this synopsis of confidentiality requirements to read and understand. This policy applies to any person performing work for, or in conjunction or collaboration with, DCAH, including classified, contract, wage and temporary employees, as well as recipients of DCAH data. All persons must comply with the following procedures.

Physical Security of Records

Accessing Confidential Information. All records containing personal identifying information within DCAH are confidential, including personnel records and patient files, both paper and electronic. Only authorized personnel may receive or review confidential documents. No confidential information shall be released to individual(s) not granted access by the ORP. Confidential information shall be accessed only by a contractor or data recipient with the authority to access such information, as delegated, and with an expressed need to access such information. Any confidential communication (written, verbal or electronic) shall be accessed on a strict need to know basis. Good judgment shall be exercised regarding access to information. All confidential information shall be used in accordance with specified contract responsibilities and/or data request stipulations.

Removing Confidential Information From Work Area. Confidential information (case reports, databases, line lists, computers, any records with identifying information in written, electronic or other format) shall only be removed from the confidential work area with prior supervisory approval and for the expressed purpose of conducting the official business of the project.

Using Confidential Information Outside Work Area. Confidential information shall be mailed in a manner that does not allow information to be revealed without opening the envelope (fold names to the inside) and envelopes shall be taped shut to ensure security. Any confidential information in use outside the offices of DCAH shall be appropriately safeguarded and shall remain the responsibility of the contractor/data recipient until such information is delivered or returned to DCAH offices.

Locking and Shredding Confidential Information. Any documents containing patient identifiers shall be secured in a locked file cabinet or drawer at the end of the business day. Any documents with identifying information that are no longer needed shall be shredded.

Disclosure

Telephones and Faxes. Confidential information should not be given out over the telephone without first confirming that the recipient is allowed access to this information. Confidential information shall not be left over voice mail. Confidential information shall be faxed with caution. Confidential information shall not be transmitted via e-mail.

Subpoenas. All subpoenas and other legal papers requesting the disclosure of confidential information served to any work unit requesting DCAH data shall be referred to the DCAH Director for consultation with the Attorney General's Office.

Virginia Freedom of Information Act. Patient level data collected under Section 32.1. -64.2, 32.1-69.2, 32.1-67.1 or 32.1-69 of the *Code of Virginia* shall be exempt from the provision of the Virginia Freedom of Information Act. This information is considered confidential. "No report published by *[a]* nonprofit organization, the Commissioner, or other person may present information that reasonably could be expected to reveal the identity of any patient. Publicly available information shall be designed to prevent persons from being able to gain access to combinations of patient characteristic data elements that reasonably could be expected to reveal the identity of any patient." (*Code of Virginia,* Section 32.1. -276.9). Release of any statistical information shall follow the "Rule of Three." Any cell with a sample size of less than three will not be revealed in order to avoid disclosure of information that may identify an individual.

Electronic Security

Login IDs, Passwords, Computers. All logon IDs and passwords that relate to DCAH confidential data shall be safeguarded, and passwords shall not be revealed to others. Always exit any confidential databases when not in use. Passwords should never be saved to your computer. Checking the box "save this password in your password list", located on the password pop-up window, is a security violation. Access to databases on computers, including laptops, shall be password protected. Passwords for CCC-SUN, VISITS, and LeadTrax shall be changed every thirty days. If the password is not used within 90 days, then the account is deactivated.

Printed Materials, Emails, Faxes. Do not print materials with identifying information on general use or unprotected printers. Do not send confidential information via e-mail. E-mail is not secure and may be seen by more people than the intended recipient. When faxing confidential material, notify the intended recipient immediately prior to sending the information. Remove disease identifiers prior to faxing.

Data Deletion. Custom databases and files with name identifiers on individual workstations; laptop computers and diskettes shall be deleted immediately upon completion of projects requiring this information. Before computers are reassigned or designated as surplus, data from the computers shall be stored on CD or disk under lock by the project manager or designee and deleted from the computer's hard drive.

PC-related Surplus, Redistribution and Disposal. Any PC-related equipment, i.e. desktops, laptops, servers, etc. tagged for state surplus or redistribution shall first be reviewed by the OFHS information system technician to ensure confidential data is absent from the hard drive. Desktop PCs are either stripped of their hard drives or have a low level format performed using DOS. If a desktop PC is being redistributed to other staffs within DCAH, a check is performed to ensure confidential data is absent from the machine. When disposing of a $3^1/_2$" diskette, the sliding metal cover must be removed from the diskette. An object such as a letter opener or pen/pencil must be used to punch a hole through the data sleeve inside the plastic casing. Scissors or a shredder must be used to destroy old $5^1/_4$" floppy diskettes.

WHEN IN DOUBT, ASK FOR GUIDANCE <u>BEFORE</u> SHARING INFORMATION.

Consequences

DCAH Employees. Violations of confidentiality and disclosure policies are subject to disciplinary action set forth in the Standards of Conduct and Performance and/or prosecution under the law as set forth in the *Code of Virginia*, Chapter 2, Title 32.1 and other applicable regulations.

DCAH Contractors, Data Users, and Data Recipients. This confidentiality policy shall be reviewed and signed annually. By signing this Statement of Confidentiality, the DCAH contractor, data user, and data recipient acknowledge an understanding of the confidentiality policies of DCAH and agree to abide by such policies. In addition, the DCAH Contractor, Data User, and Data Recipient acknowledge that the regulations governing the confidentiality and disclosure of information related to Child and Adolescent Health are mandated by the *Code of Virginia* and that the regulations are therefore not necessarily limited to current employees of DCAH.

SECTION 2. PHYSICAL SECURITY

Building Access

Virginia Department of Health Accessibility

Most offices of the Virginia Department of Health (VDH) are housed in Main Street Station (MSS), 1500 East Main Street, Richmond, Virginia. Building access is monitored via an employee entry card system. Individual employees are to use their own card to access the building and not "piggyback" with another employee upon entering the building. The access card can be used at any time of the day and must be used to enter the building at all entrances. Visitors must enter by one entrance and sign in with the building security officer.

Division of Child and Adolescent Health Accessibility

DCAH is housed in four suites that are located inside MSS.

Confidential Information

Access to areas where confidential information is used by the contractor/data recipient should be limited to authorized personnel only.

SECTION 3. COMPUTER SECURITY

Desktops and Laptops [10]

All users of DCAH confidential data are responsible for protecting their own workstation and laptop, if applicable, from misuse. This responsibility includes the protection of diskettes and passwords/codes that would allow access to confidential information or data. All data-related papers and diskettes must be stored appropriately when staffs are away from their work areas. This includes proper filing at the end of a workday and protection of workstation and computer during short absence from them during work hours.

Virus Protection [11]

All users of DCAH confidential data are advised to use virus protection for protecting their own desktop and laptop. A link to anti-virus software is available from the VDH Intranet home page, and as needed, assistance is provided to staffs by an information systems technician on downloading virus definition updates. Anti-virus software is running continuously on DCAH computers each day. The downloading of virus definitions to the desktop and laptop are set to occur daily.

Network Accessibility

LAN Operation. The CCC-SUN, VISITS, and LeadTrax information systems are hosted and maintained by Welligent, LLC, which utilizes the Children's Health System (CHS) Novell 4.11 network for its local area network (LAN) operations. All access to the CHS network is controlled through the use of unique passwords. Intruder lockouts occur once an incorrect password has been attempted several times. Access to Welligent, LLC confidential data, housed in a Sun E5500 in Norfolk, are stored on this network; however, user rights to such files have been restricted and are only accessible by authorized Welligent, LLC staff.

Passwords. CHS network passwords are managed by the Information Services Department at Children's Hospital of the King's Daughters. Only the information systems administrator at CHKD can reset a user's CHS account. With a few exceptions, CHS user accounts are limited to one login at a time. This helps to control PCs being left connected to the network inadvertently, thus decreasing likelihood of unauthorized access.

Passwords for required Welligent, LLC network processes are maintained by Welligent, LLC systems administrator. Only the above individual and a back-up technician will know these passwords. In the event any staffs terminate employment with Welligent, LLC, or the password list is considered to be have been tampered, the passwords and the

[10] Information System Audit Item 23: Provide evidence the client desktops/laptops have physical security when authorized individuals are not available at the desktop/laptop.

[11] Information System Audit Item 26: Provide evidence the remote sites have been advised to use virus protection on the client desktop/laptops.

location of the information will be immediately changed. Any changes to network user accounts and/or associated user rights must be approved by the Director of Welligent, LLC.

Database Accessibility

Contingency Plans [12]

CCC-SUN, VISITS, and LeadTrax information systems used by DCAH are maintained on Welligent, LLC server and network. Welligent, LLC has a plan for contingencies so if something goes wrong with the server or network, DCAH can continue business.

Organization's Standardized Roles [13]

Database files for CCC-SUN, VISITS, and LeadTrax information systems are structured with rights limited to staffs whose jobs require such access. A diverse discipline user committee developed standardized roles for each database. The Director of the DCAH, who serves as the Overall Responsible Party (ORP), has approved and certified that applications' standardized roles are appropriate and based upon information security principles.

CCC-SUN User Roles. The user roles for CCC-SUN are presented in Table 1.

Table 1. CCC-SUN User Roles

Ability to read, select, and run reports.	CCC-SUN VIEW
Ability to create, insert, read, select, run reports, and update data for patients of only one designated CCC center which is the center in which the person is employed. Ability to transfer patient data to another CCC Center	CCC-SUN CENTER USER
Ability to create, insert, read, select, run reports, update data and delete data for all centers statewide. Ability to transfer patient data to another CCC Center	CCC-SUN STATEWIDE ADMINISTRATOR
Ability to create, insert, read, select, run reports, update data and delete data for patients of only one designated center. Ability to transfer patient data to another CCC center.	CCC-SUN CENTER ADMINISTRATOR

[12] *Information Systems Audit Item 12: Provide evidence of the existence of written policies and procedures for contingencies, a plan.*

[13] Information Systems Audit Item 14: Provide evidence that management has approved and certified that organization's standardized roles are appropriate and based upon information security principles.

VISITS User Roles. The user roles for VISITS are provided in Table 2.

Table 2. VISITS User Roles

Ability to create, insert, read, select, update data and run reports only for those patients reported by a user from same hospital	VISITS Hospital User
Ability to create, insert, read, select, update data, run reports and delete data for all hospitals statewide	VISITS Administrator

LeadTrax User Roles. The user roles for LeadTrax are provided in Table 3.

Table 3. LeadTrax User Roles

ACCESS	ROLE ID
Ability to create, insert, read, select, update data, run reports, pull extracts, and delete data	LeadTrax Administrator
Pull extracts from database for analysis	Analyst
View patient and environmental data and run queries and reports (locality specific)	Director
View and edit child data both clinical and environmental, run reports (locality specific)	Case Manager
View child lab data and view and edit environmental data, run reports (locality specific)	Environmental Specialist
Ability to create, insert, read, select, run reports, and update data for patients (locality specific)	Program Support

For CCC-SUN, VISITS, and LeadTrax individual user rights are set up by the DCAH program director for the database application and the user accounts are set up and maintained by Welligent, LLC. Any changes to user accounts and/or associated user rights must be approved by the DCAH program director for the database application.

Process For User Access, Change, and Termination [14, 15, 16, 17]

1. **New User Status.** Persons requesting new user status go to the CCC-SUN and VISITS public page to obtain copies of the *Information Systems: Security and Confidentiality Policies, Procedures, and Standards* and the Information Systems Security Access Agreement (see Attachments) and Points of Contacts (See Attachments). LeadTrax users will access the above documents on the VDH Internal Web page under the security section.
   a. Applicant completes all information, signs both the Access Agreement and the Certificate of Receipt for the *Information Systems: Security and Confidentiality Policies, Procedures, and Standards,* faxes both to the Project Manager for CCC-SUN, VISITS, or LeadTrax and mails originals to the Project Manager.
   b. Project Manager signs the Access Agreement and faxes it to Welligent, LLC to create a user account and assign temporary password.
   c. Project Manager keeps a file of all Access Agreements and Certificate of Receipts.

2. **Change in User Name or Role**
   a. User completes a new Access Agreement and Certificate of Receipt, faxes both to the Project Manager, and mails originals to the Project Manager.
   b. User updates the "My Profile" information on CCC-SUN/VISITS/LeadTrax message center.

3. **User Termination.** User access to VISITS, CCC-SUN, and LeadTrax will be terminated when:
   a. The Project Manager is notified that the user is no longer employed by the facility or no longer has a need to access the database.
   b. User has not accessed the system in 90 days
   c. User sanctioned for a breach of security

4. **CCC-SUN, VISITS, and LeadTrax Security Committees.** Members of the CCC-SUNS, VISITS, and LeadTrax Security Committees are knowledgeable about the State Health Commissioner's policy on Information Systems Security Requirements dated Fri, 07 Apr 2000 16:01:13 -0400 by e-mail.

5. **Vendors, Project Managers, and ISSOs.** The vendor—Welligent, LLC—and the information systems managers (Project Managers and Information Systems Security

[14] Information Systems Audit Item 15. Provide evidence that the organization has establish a process for end-users to request access and privileges, management validates/invalidates the request, application/data owner validates/invalidates management's approvals, information systems security manager implements application/data owners implementation instructions for establish accounts and privileges, and the termination process is established to change or remove accounts and privileges.

[15] Information Systems Audit Item 16. Provide evidence that an account and privileges assignment / unassignment process have been established and documented.

[16] Information Systems Audit Item 17. Provide evidence that application's Access Request Procedures include the agency's Confidentiality/Privacy Policy and Agency Information Systems Security Agreement.

[17] Information Systems Audit Item 18. Provide evidence that the access authorization records are maintained by the systems security officer. (Be aware that State Security Policy states that access authorizations etc. should be place in personnel records).

Officers) are knowledgeable about the Information Systems Security Policies, Standards, Best Security Procedures, and Standards of the Virginia Department of Health.

6. **All Parties**. DCAH, information systems employees, contractors, data users and data recipients are aware of the access, change and termination process and have assigned their employees to tasks based upon the "separation of duties" principles.

7. **All Parties**. DCAH information systems data users certify that they understand their responsibilities for and during the use of information systems.

8. **All Parties**. DCAH information systems data users certify that they understand their confidentiality responsibilities when learning or working with confidential information, e.g. patient identifiable data.

9. **Data Users.** DCAH information systems data users certify that access is requested only on the basis of "needs to know" to accomplish authorized work.

10. **Supervisors**. Immediate supervisor[18]
    a. Certifies that user is requesting roles or tools based upon "needs to know" and "separation of duties".
    b. Ensures that the required forms are fully completed (Security Access Agreement and the Certificate of Receipt).
    c. Notifies VDH Project Manager and Welligent, LLC within 24 hours when the user's services are changed or terminated.

11. **Project Managers.** VDH Project Manager[19] or their delegate
    a. Certifies that user is requesting roles or tools based upon "needs to know" and "separation of duties.
    b. Ensures that the required forms are fully completed (Security Access Agreement and the Certificate of Receipt)

12. **Data Owners.** The Data Owner[20] or their delegate certifies that it is appropriate for the user to have access to specific data or data tools and ensures that the Security Access Agreement and the Certificate of Receipt are completed.

[18] Immediate supervisor: The immediate supervisor is the best person to verify that the employee is assigned to access the system, that the employee has the need--to-know about specific data and that the employee has the need for a specific tool to accomplish the assignment.

[19] Project Manager: The Project Manager is a person who is responsible for a specific program for the Virginia Health Department. Each VDH information system (VISITS Hearing, VISITS Virginia CARES, CCC-SUN), LeadTrax has a Project Manager.

[20] Data Owner: The Data Owner is the person who is responsible for data integrity, which is that data is complete, accurate, and timely. For example the State Health Commissioner is responsible for the integrity of all data of the Virginia Department of Health. Since it is impractical for the State Health Commissioner to ensure the data integrity without assistance of others, then the responsibility is delegated to the management that is closest to that ability to ensure integrity. The management who are delegated the responsibility ensure data integrity by various means: 1) they provide oversight that their employees add, change, and delete data appropriately, 2) they provide oversight that the application are function as is required, 3) they are ensuring that the access privileges are given end-user based upon "separation of duties principles," "need-to-know principles" and "least-privileges principles" and 4) they provide oversight that

13. **Host ISSO**. Host Information Systems Security Officer is responsible for implementing the Data Owner's instructions based upon "least-privileges" principle and for raising any potential access control weaknesses. The Host Information Systems Security Officer is in compliance with:
    a. Federal Information Systems Security Laws, Policies, Standards, Directives, Regulations and Guidelines.
    b. State Information Systems Security Laws, Policies, Standards, Directives, Regulations and Guidelines.
    c. VDH Information Systems Security Laws, Policies, Standards, Directives, Regulations and Guidelines.
    d. HIPAA Proposed IT Security Regulations.

    The Project Manager should have an alternative confirmation source when VDH users leave their employment, e.g. personnel notification, payroll notification, to identify people who left their employment, but the immediate supervisor or program manager failed to notify the security officer.

Systems Perimeter: People – Security Awareness and Training [21, 22, 23, 24]

Awareness and Training for All Parties. WebEx[25] training conducted for users of the VISITS, CCC-SUN, and LeadTrax includes information about security awareness and password management. The Information Systems Security Access Agreement contains statements about security and the need for awareness of all applicable Federal, Commonwealth and VDH policies, Procedures, and Standards. Periodic information is available to users in the following ways:

- Posted on the VISITS, CCC-SUN, and LeadTrax main pages.
- Posted under VISITS, CCC-SUN, and LeadTrax Frequently Asked Questions.
- Sent to users via the VISITS, CCC-SUN, and LeadTrax Announcement Board.
- Sent to users via My Messages, the VISITS, CCC-SUN, and LeadTrax internal messaging system.

DCAH employees will be periodically updated on systems security awareness information as is necessary to maintain compliance with Federal, state, VDH and HIPAA laws, policies, standards, directives, regulations and guidelines.

the data custodians (a.k.a. information system security officers) are monitoring the application and operating systems. Security is implemented appropriate for the protection of the data.

[21] Information Systems Audit Item 123. Provide evidence that there is security awareness training and periodic security reminders.

[22] Information Systems Audit Item 124: Provide evidence of user education in importance of monitoring login success/failure, and how to report discrepancies.

[23] Information Systems Audit Item 126: Provide evidence that technical maintenance personnel are trained in systems security

[24] Information Systems Audit Item 125: Provide evidence of user education in password management.

[25] WebEx™ provides multimedia business communications services that enable Web conferencing, video conferencing, teleconferencing—all accessed through an Internet browser.

Policy, Procedures, and Standards Manuals: CCC-SUN and VISITS. The DCAH document *Information Systems: Security and Confidentiality Policies, Procedures, and Standards* and the Information Systems Security Access Agreement are available on the VISITS and CCC-SUN public pages and the VISITS and CCC-SUN Web sites as downloadable documents. The LeadTrax documents are available for download on the VDH Internal Web site under Security and posted on the LeadTrax Web site.

Vendors. The vendor, Welligent, LLC, is the information systems developer and information systems management contractor for CCC-SUN, VISITS, and LeadTrax and is responsible for:

- Monitoring login success and failure.
- Reporting of discrepancies.
- Information systems security training.

PC Workstation Accessibility [26, 27]

Leaving Computer. All PCs within DCAH are required to be turned off at the end of each workday. Staffs with PCs that access confidential information shall ensure that such databases are closed and/or the PCs are turned off when leaving the work area for periods of time such as lunch breaks. When PCs are left unattended for short durations such as bathroom breaks, monitors will have password protected screen savers with no more than 15 minute idle time setting on desktop/laptops for the prevention of data leakage.

Suspicious Activity. All DCAH staffs are required to report any suspicious activity involving their PC immediately to their supervisor. In such instances, DCAH management may decide to include a Basic Input Output System (BIOS) password on the PC as an added security precaution.

BIOS Password. Any PC in a non-secure location used to access or utilize confidential information should be protected by a BIOS password. Also, database access shall only be performed while physically located at the PC. The PC monitor must also be situated such that persons other than the user cannot easily view it.

[26] *Information System Audit Item 24: Provide evidence that end-user have been advised that client workstations are located in a place to eliminate or minimize the possible unauthorized visual eavesdrop to information.*

[27] *Information System Audit Item 25: Provide evidence that offices/district infosec officers have received a policy to implement screen savers on desktop/laptop for the prevention of data leakage.*

SECTION 4. DATA-RELATED SECURITY AND CONFIDENTIALITY

Authorized Data & Database Usage

User Accounts. User accounts for confidential databases are maintained by the Host Information Systems Security Officer and the Project Manager. Access to confidential surveillance information is limited to staffs who require such information to perform their work activities. User accounts are deleted immediately upon termination of an employee's need to access a confidential database system.

Non-DCAH Personnel. Personnel outside DCAH confidential units may gain access to confidential information only if (1) the request for such information has been authorized by the Overall Responsible Party (ORP) and is deemed a justifiable public health need and (2) the request does not compromise or impede surveillance or other confidential DCAH activities.

Sharing of Data. Identifying information from DCAH databases shall be shared with other disease registries only after a thorough review by the ORP (see Section 1. Responsibility Parties, ORP.). Sharing of data shall be consistent with *Code of Virginia* §§ 32.1-127.1:03 and 32.1-127.1:04. The ORP will limit such activities to other registries that can demonstrate a justifiable need for the data. The decision to allow such activity will also be weighed against the benefits and risks of allowing access and upon certification that the level of security established by the other registry is at least equivalent to the standards described in this document. The final decision regarding the sharing of registry data and data matches rests upon the ORP.

Photocopying and Printing of Confidential DCAH Surveillance Data

Printing Materials. DCAH information systems contractors, data users, and data recipients shall not print materials with identifying information on general use or non-secure printers. All printing of such documentation shall occur within the confines of a secure office and the print job shall be removed from the printer immediately upon completion. Any unnecessary copies shall be shredded immediately, as well as originals once its use is obsolete.

Photocopying Materials. Photocopying of confidential information should occur only within the confines of a secure office and should be removed from the photocopier immediately upon completion. Only the mandatory number of copies of such information shall be photocopied. Any extra or test copies shall be shredded immediately upon completion.

Emailing Data

Data transfers to or from contractors are only performed via email if personal identifiers are nonexistent. Any data including personal identifiers approved for analysis by a contractor are hand-delivered without easily identifiable disease codes. Hard copy data transfers including personal identifiers should not include identifiable disease information and should be hand-delivered to applicable personnel inside envelopes without specific indication of the nature of the data. DCAH data managed by contractors are subject to all standards within this document. Any dissemination of information resulting from data managed by contractors shall be reviewed by DCAH staffs prior to release. Sufficient time should be allotted for this review procedure. A copy of all final products shall be provided to DCAH staffs at the time of dissemination. All contractors shall sign applicable DCAH protocols regarding data release and confidentiality on an annual basis.

Release of Data to Non-DCAH Personnel

Access to any surveillance information for research purposes (other than routine surveillance) must be contingent upon a demonstrated need for the data, possible Institutional Review Board (IRB) approval, and the signing of confidentiality and data release agreements. As covered within the data release agreement (see attachment), such data are solely for the explicit use specified. Once the intended use of the data has been completed, all data must be destroyed or returned to DCAH. No additional data extrapolations or usage is permitted, unless otherwise approved by the ORP.

The “Rule of Three”

In order to protect the confidentiality of persons reported within DCAH information systems, DCAH follows a “Rule of Three” information security principle. The DCAH Rule of Three requires that there shall be no dissemination of a table data cell to the general public that involves (1) a particular demographic characteristic containing less than three or (2) locality or region-specific data containing cells less than three —unless the data cell represents one entire year’s worth of data. Likewise, if the contents of a suppressed cell in a table could be determined by simple mathematical calculations of the non-suppressed rows or columns, then the additional rows or columns would also need to be suppressed. Any uncertainty regarding the release of such data must be clarified by supervisors.

Note: The DCAH Rule of Three is the same Rule of Three that is followed by the VDH Division of STD/AIDS as recommended by the Centers for Disease Control and Prevention.

Security Breaches

Reporting [28]

Any suspected breach of security, whether intentional or unintentional, shall be reported to DCAH immediately upon discovery of said incident. The contractor or information systems user is responsible for immediately informing the Project Manager of the details regarding the incident and documenting in writing the circumstances of the occurrence. The written documentation of the breach shall be faxed, emailed or mailed to the Project Manager not later that 2 business days following the incident. Written notification shall include:

1. A brief description of the breach,
2. Impact of the breach
3. Onsite notification of supervisor
4. User's name and location

Response [29]

Upon notification of a suspected breach of security, the Project Manager will immediately notify the following individuals of the suspected breach.

1. Project Manager's Supervisor
2. DCAH Director
3. Host Information Systems Security Officer
4. Agency Information Systems Security Officer
5. VDH System Security Officer
6. Agency Internal Audit Director

Working in collaboration, this team will immediately begin an investigation of the suspected breach. All material related to the investigation shall be marked sensitive and confidential and will not be public information until the investigation is complete. The investigation will include:

1. An assessment of the cause(s) of breach.
2. Consultation with Welligent, LLC regarding the breach.
3. Identification and implementation of strategies to remedy future occurrences.
4. If warranted, notification and consultation with the Attorney General's office to determine if the breach warrants reporting to appropriate law enforcement agencies.
5. The Project Manager and the Agency Information Systems Security Officer will maintain a record of suspected breaches.

Sanctions [30]

Project Manager and DCAH Director. If a breach is determined to have resulted in the release of confidential information about one or more individuals, the Project Manager

[28] Information Systems Audit Item 118: Provide evidence of incident reporting procedures.

[29] Information Systems Audit Item 119: Provide evidence of incident response procedures.

[30] Information Systems Audit Item 120: Provide evidence of security violations sanctions policy.

will maintain responsibility for reporting the incident to the Director of the Division of Child and Adolescent Health for determination of disciplinary action.

Reporting Breach of Security. Any suspected breach of security shall be reported to DCAH immediately, including both inadvertent and advertent breaches. DCAH information systems contractors, data users, and data recipient are responsible for immediately informing DCAH management of details regarding the incident and documenting the occurrence. DCAH or OFHS management will immediately investigate the suspected breach to assess causes, implement remedies and through consultation with the Attorney General's office, determine whether the breach warrants reporting to appropriate law enforcement agencies.

Level of Sanctions. Sanctions are based on the level of breach and may include, but not be limited to, the following:

- Terminating access to information systems.
- Reporting breach to law enforcement.
- For state employees, implementing disciplinary action according to (1) Commonwealth of Virginia, *Information Technology Security Standard* and (2) Commonwealth of Virginia, *Standards of Conduct*.

SECTION 5. RAPID COMMUNICATIONS

Any confidential communication (written, verbal or electronic) shall be shared with other persons on a strict need to know basis, as designated in the DCAH Data Recipient Agreement (see Attachments).

Postal/Mailing Services

Incoming

Mailing Envelope. Confidential information should be mailed to DCAH in a manner that does not allow information to be revealed without opening the envelope. The number of documents per envelope shall be kept to a minimum. Envelopes shall be taped shut as added security.

Labeling Envelope. All mail incoming to DCAH is received within room 137. Incoming mail with confidential information should be sent to DCAH marked *Confidential, To Be Opened By Addressee Only* and shall be sent at least via first class.

Outgoing

Mailing Envelope. Confidential information should be mailed from DCAH in a manner that does not allow information to be revealed without opening the envelope. The number of documents per envelope shall be kept to a minimum. Envelopes shall be taped shut as added security.

Labeling Envelope. All such confidential information mailed from DCAH shall be marked *Confidential, To Be Opened By Addressee Only* and shall be sent at least via first class.

Telephone

Incoming

Incoming Calls. Assistance with sharing confidential information through incoming calls shall only be completed if the DCAH staff is 100% confident of the identity of the caller and he/she is an authorized recipient of such confidential information.

Call Back Verification. Uncertainty regarding the identity of a caller should be verified via a call back procedure and/or discussion with appropriate personnel.
If a call back verification is performed, DCAH staffs shall not acknowledge this procedure to the caller. The caller's name, location and telephone number should be obtained and the caller informed that a DCAH staff would return their call as quickly as possible. When the call back procedure is performed, DCAH staffs should receive immediate acknowledgement of the caller's location, etc.

Uncertainty. Any uncertainty regarding the caller's location or authorization to receive such information should be immediately forwarded to the DCAH staff's supervisor. DCAH staffs shall not release any information if unsure of the legitimacy or authorization of the caller. In general, all such calls should be forwarded to the DCAH staffs who performs this type of task routinely.

Outgoing

Outgoing Calls. Confidential information is shared with persons outside DCAH on a strict need to know basis and performed only in secure areas. In general, such calls are performed as a result of follow up to an inquiry or for updates to current morbidity reports and surveillance activities. Sharing confidential information through outgoing calls shall only be completed if the DCAH staff is 100% confident in the identity of the recipient of the call and he/she is an authorized recipient of such confidential information.

Uncertainty. DCAH staffs shall not release any information if unsure of the legitimacy or authorization of the recipient.

Voice Mail. Messages with identifying patient information shall not be left on voice mail systems.

Responsibility. Unless otherwise instructed by supervision, these types of calls should only be completed by DCAH staffs who routinely perform this type of task.

Electronic

Facsimile (Fax)

To DCAH. Confidential information shall be faxed with caution, using the utmost discretion. A telephone call should immediately precede any incoming facsimile that contains confidential information, such that the appropriate DCAH staff is mindful of the document being faxed. The DCAH staff recipient of such a call should (1) verify the appropriate fax number being used by the caller, and (2) await the facsimile completion and immediately remove such documentation from the fax machine. If incoming faxes are not received within an expected time frame, the DCAH staff awaiting the facsimile should contact the sender. Completed facsimiles with confidential information shall not be left on fax machines unattended. All facsimile transactions involving confidential information should be received through a DCAH fax machine located in a secure area.

From DCAH. Outgoing facsimile transactions from DCAH shall follow the same standards as above. In addition, disease coding shall be used to reduce the likelihood of comprehension in the event the facsimile is received by unauthorized personnel. A fax cover sheet excluding identity of DCAH title should also be used. Fax machines used to send out confidential information should be programmed to indicate "Dept. of Health" on the top line of the faxed document, not "Division of Child and Adolescent Health." The facsimile transmission sheet should have a statement such as the following:

> *This facsimile transmission contains confidential or legally privileged information that is intended only for the use of the individual or individuals named on the transmission sheet. If you are not the intended recipient, you are notified hereby that any disclosure, copying distribution, or the taking of any action in reliance on the contents of this facsimile transmission is strictly prohibited. If you have received this communication in error, please call me collect immediately so that I can arrange for the return of the documents to me at no cost to you.*

Electronic Mail (E-mail)

Confidential information shall not be transmitted via e-mail. E-mail is not secure and may be seen by more people than the intended recipient. Routine data requests minus personal identifiers may be sent using e-mail; however, the rule of three shall apply, where appropriate. MS Word and MS Excel documents with passwords can be sent as attachments to e-mail messages until such time that VDH implements PKI, digital encryption and digital signatures.

ATTACHMENTS

Virginia Department of Health
Division of Child and Adolescent Health

Data Request Form

Requests for non-routine data, including any request for DCAH data sets, data matches or patient identifying information, must be submitted in writing to DCAH for data release consideration. Virginia Department of Health employees are exempt from this process; however, clear explanation should be provided regarding proposed data needs. Health department contractors or collaborators are not considered health department employees. Submission of this request does not guarantee approval and release of Division of Child and Adolescent Health data.

Submission
Date:________/________/___________

Requestor:______________________________Phone:_______-_______-_____________

Title:__________________________________Fax: _______-_______-_____________

Organization:____________________________Email:_____________________________

Purpose of Request:

____
____
____
____

Data Requested: [include timeframe(s), disease(s), demographics, etc]:

____
____
____
____

Data Use Methodology [if a research study/project, attach complete study design proposal and notice of Institutional Review Board (IRB) approval]:

____
____
____
____

Description of Data Protection Mechanisms [staff accessibility, electronic security, locks, etc]:

____
____
____
____

At the conclusion of this project, the data will be: *(check one)*

□ Returned to the Division of Child and Adolescent Health
□ Destroyed

Method: ____
____

____
Signature of Requestor

cc: Data Recipient
Director of Statistics & Data Mgmt
File

Virginia Department of Health
Division of Child and Adolescent Health

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment

Data Recipient Agreement

The undersigned hereby agrees to the following terms and conditions relating to any data requested of the Virginia Department of Health Division of Child and Adolescent Health:

A. The information obtained through this data request will be used only for surveillance of treatment, care and disease trends, prevention strategies or for statistical purposes in medical and health research.

B. No data shall be released or published by the data recipient in any form potentially identifying a particular individual, physician, hospital or other reporting source. Data subsets without personal identifiers must comply with confidentiality standards based on data cell size, i.e. the "Rule of Three" as described by the Division of Child and Adolescent Health.

C. The data recipient shall sign the Division of Child and Adolescent Health Security & Confidentiality Policies, Procedures, and Standards. These standards shall be renewed every 12 months, as applicable.

D. Any identifying information in this data request shall not be used as a basis for legal, administrative, or other actions that may directly affect those particular individuals or establishments as a result of their specific identification in this project.

E. Information obtained through this request shall not be distributed to anyone else, including subcontractors and third-party analysts. The data shall not be used for any project other than the intended use specified in the data request.

F. Unless specified and approved through the original proposal, no "follow-back" investigations to obtain additional information from physicians, hospitals, or patients shall be undertaken.

G. All data received from the Division of Child and Adolescent Health shall be returned to the Division or disposed of by an approved method at the end of the project. The data recipient shall state the method of return or disposal prior to receipt of the data.

H. Any suspected or confirmed breach of data confidentiality or security shall be immediately reported to the Director of the Division of Child and Adolescent Health.

I. Draft versions of all work products shall be sent to the Division of Child and Adolescent Health for review prior to any distribution. Sufficient time should be allotted to allow for review and comments prior to distribution.

J. A copy of all final work products resulting from use of the data shall be sent to the Division of Child and Adolescent Health prior to or at the time of distribution.

As a recipient of data from the Virginia Department of Health Division of Child and Adolescent Health, I agree to abide by the above stipulations.

Signature: ______________________________ Date: ____________________

Organization: ____

cc: Data Recipient
File

Virginia Department of Health
Division of Child and Adolescent Health

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment

Information Systems Security Access Agreement: CCC-SUN

This form grants authorization to individuals to access the Care Connection for Children System Users Network (CCC-SUN) database. The database owner, the Division of Child and Adolescent Health (DCAH) of the Virginia Department of Health (VDH), must grant specific authorization to those who wish to access the database system. Without this authorization, no individual has any general authority to view, insert, delete, or update CCC-SUN data. The criteria used to determine access should be based on a minimum privilege needed by the individual to perform their job duties.

Access has been granted to me by VDH as a necessary privilege in order to perform my authorized job functions. As a user of the Department of Health information systems, I understand and agree to abide by the CCC-SUN Security Policy and the following terms that govern my access to and use of the system. All logon IDs and passwords shall be safeguarded, and passwords shall not be revealed to others. I am prohibited from using or knowingly permitting use of any logon ID's and passwords for any purposes other than those required to perform my authorized job functions. I agree to change passwords immediately if they are compromised. I understand that I am responsible for all activities performed under my assigned logon ID. If the system is misused under my password, I am responsible.

I will not disclose any confidential, restricted or sensitive data to unauthorized persons. I will not disclose information regarding any access control mechanism of which I have knowledge.

I agree to abide by all applicable Federal, Commonwealth of Virginia and VDH agency policies, procedures and standards that relate to the security of the VDH information systems and the data contained therein.

If I observe incidents of noncompliance with the terms of this agreement, I am responsible for reporting them to the information security officer and management of my employing agency as well as management of VDH.

I give consent to the monitoring of my activities on VDH information systems.

By signing this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in the termination of my access privileges. I have read and have had an opportunity to ask questions and obtain responses in order for me to understand the content of the DCAH document, *Information Systems: Security and Confidentiality Policies, Procedures, and Standards.*

Employee's Full Name:

Employer Name: ______________________________

Work Site Location (city): ______________ CCC Region: ____________ ____

Job Title: ______________________________

Phone Number: ______________ Fax Number: ______________

Email Address: ______________________________

Signature: ______________________________ Date: __________

Supervisor's Signature: ______________________ Date: __________

Supervisor's Name (Printed): ______________________________

Fax completed form to: 804-864-7723.
Mail original form to: Virginia Department of Health, James Madison Building, 109 Governor Street, 8th Floor, Richmond, VA 23219. ATTN: Division of Child and Adolescent Health/**CSHCN**

VDH Use Only: Approved CCC-SUN User Role ______________________________

Program Manager (Print): ______________________________
Signature: ______________________________ Date: __________

Revised **02/03/04**

Virginia Department of Health
Division of Child and Adolescent Health

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment

Information Systems Security Access Agreement: VISITS

This form grants authorization to individuals to access the Virginia Infant Screening and Infant Tracking System (VISITS) database. The database owner, the Division of Child and Adolescent Health (DCAH) of the Virginia Department of Health (VDH), must grant specific authorization to those who wish to access the database system. Without this authorization, no individual has any general authority to view, insert, delete, or update VISITS data. The criteria used to determine access should be based on a minimum privilege needed by the individual to perform their job duties.

Access has been granted to me by VDH as a necessary privilege in order to perform my authorized job functions. As a user of the Department of Health information systems, I understand and agree to abide by the VISITS Security Policy and the following terms that govern my access to and use of the system. All logon IDs and passwords shall be safeguarded, and passwords shall not be revealed to others. I am prohibited from using or knowingly permitting use of any logon ID's and passwords for any purposes other than those required to perform my authorized job functions. I agree to change passwords immediately if they are compromised. I understand that I am responsible for all activities performed under my assigned logon ID. If the system is misused under my password, I am responsible.

I will not disclose any confidential, restricted or sensitive data to unauthorized persons. I will not disclose information regarding any access control mechanism of which I have knowledge.

I agree to abide by all applicable Federal, Commonwealth of Virginia and VDH agency policies, Procedures, and Standards that relate to the security of the VDH information systems and the data contained therein.

If I observe incidents of noncompliance with the terms of this agreement, I am responsible for reporting them to the information security officer and management of my employing agency as well as management of VDH.

I give consent to the monitoring of my activities on VDH information systems.

By signing this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in the termination of my access privileges. I have read and have had an opportunity to ask questions and obtain responses in order for me to understand the content of the DCAH document, *Information Systems: Security and Confidentiality Policies, Procedures, and Standards.*

Employee's Full Name: ______________________________

Hospital Name: ______________________________

Hospital Location (city): ______________________________

Job Title: ______________________________

Phone Number: ______________ Fax Number: ______________

Email Address: ______________________________

Signature: ______________________ Date: __________

Supervisor's Signature: ______________________ Date: __________

Supervisor's Name (Printed): ______________________________

Fax completed form to: 804-864-7721.
Mail original form to: Virginia Department of Health, James Madison Building, 109 Governor Street, 8th Floor, Richmond, VA 23219. ATTN: Division of Child and Adolescent Health/**VEHDIP** (*if Hearing Modules User*) **or** ATTN Division of Child and Adolescent Health/**VaCARES** (*if VaCARES Module User*).

VDH Use Only: Approved VISITS User Role: ______________________

Program Manager (Print): ______________________________

Signature: ______________________ Date: __________

Revised **02/03/04**

Virginia Department of Health
Division of Child and Adolescent Health

Information Systems Security Access Agreement: LeadTrax

This form grants authorization to individuals to access the *LeadTrax* database. The database owner, the Division of Child and Adolescent Health (DCAH) of the Virginia Department of Health (VDH), must grant specific authorization to those who wish to access the database system. Without this authorization, no individual has any general authority to view, insert, delete, or update *LeadTrax* data. The criteria used to determine access should be based on a minimum privilege needed by the individual to perform their job duties.

Access has been granted to me by VDH as a necessary privilege in order to perform my authorized job functions. As a user of the Department of Health information systems, I understand and agree to abide by the *LeadTrax Information Systems Security and Confidentiality Policies and Procedures* and the following terms that govern my access to and use of the system. All logon IDs and passwords shall be safeguarded, and passwords shall not be revealed to others. I am prohibited from using or knowingly permitting use of any logon ID's and passwords for any purposes other than those required to perform my authorized job functions. I agree to change passwords immediately if they are compromised. I understand that I am responsible for all activities performed under my assigned logon ID. If the system is misused under my password, I am responsible.

I will not disclose any confidential, restricted or sensitive data to unauthorized persons. I will not disclose information regarding any access control mechanism of which I have knowledge.

I agree to abide by all applicable Federal, Commonwealth of Virginia and VDH agency policies, procedures and standards that relate to the security of the VDH information systems and the data contained therein.

If I observe incidents of noncompliance with the terms of this agreement, I am responsible for reporting them to the information security officer and management of my employing agency as well as management of VDH.

I give consent to the monitoring of my activities on VDH information systems.

By signing this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in the termination of my access privileges. I have read and have had an opportunity to ask questions and obtain responses in order for me to understand the content of the DCAH document, *Information Systems: Security and Confidentiality Policies, Procedures, and Standards.*

Employee's Full Name: ______________________________

Employer Name: ______________________________

Work Site Location (city): ________________ Health District: ______________

Job Title: ______________________________

Phone Number: ________________ Fax Number: ________________

Email Address: ______________________________

Signature: ______________________________ Date: ____________

Supervisor's Signature: ______________________ Date: ____________

Supervisor's Name (Printed): ______________________________

Fax completed form to: 804-864-7723.
Mail original form to: Virginia Department of Health, James Madison Building, 109 Governor Street, 8th Floor, Richmond, VA 23219. ATTN: Division of Child and Adolescent Health/**Lead-Safe Virginia**

VDH Use Only: Approved LeadTrax User Role ______________________

Program or Database Manager (Print): ______________________

Signature: ______________________________ Date: ____________

Revised 02/03/04

Points of Contact—CCC-SUN

Security Issues

Name	Phone Number	Fax Number	E-Mail Address
Nancy Bullock CSHCN Program Director, DCAH, VDH	(804) 864-7706	(804) 864-7723	nancy.bullock@vdh.virginia.gov
Joanne Boise Director DCAH, VDH	(804) 864-7685	(804) 864-7722	joanne.boise@vdh.virginia.gov
Michelle McCranie Security Officer Welligent, LLC	(757) 668-6582	(757) 668-6575	mmccranie@welligent.com

System Issues

Name	Phone Number	Fax Number	E-Mail Address
Help Desk: Aprielle Barclift Welligent, LLC	(757) 668-6586	(757) 668-6575	abarclif@welligent.com
Technical Assistance: Charles Sutelan CEO Welligent, LLC	(757) 668-6428	(757) 668-6575	csutelan@chkd.com

Revised **02/03/04**

Points of Contact—VISITS Hearing

Security Issues

Name	Phone Number	Fax Number	E-Mail Address
Pat Dewey Virgina Early Hearing Detection and Intervention Program Manager DCAH, VDH	(804) 864-7713	(804) 864-7721	pat.dewey@vdh.virginia.gov
Nancy Ford Director, Pediatric Screening and Genetics, DCAH, VDH	(804) 864-7691	(804) 864-7721	nford@vdh.state.va.us
Michelle McCranie Security Officer Welligent, LLC	(757) 668-6582	(757) 668-6575	mmccranie@welligent.com

System Issues

Name	Phone Number	Fax Number	E-Mail Address
Help Desk: Aprielle Barclift Welligent, LLC	(757) 668-6586	(757) 668-6575	abarclif@welligent.com
Technical Assistance: Rick Hasson Sr. Programmer Welligent, LLC	(757) 668-6450	(757) 668-6575	rhasson@welligent.com

Revised **02/03/04**

Points of Contact—VISITS-VaCARES

Security Issues

Name	Phone Number	Fax Number	E-Mail Address
Sharon Williams Virginia Genetics Program Manager DCAH, VDH	(804) 864-7712	(804) 864-7721	sk.williams@vdh.virginia.gov
Nancy Ford Director, Pediatric Screening and Genetics Services DCAH, VDH	(804) 864-7691	(804) 864-7721	nancy.ford@vdh.virginia.gov
Michelle McCranie Security Officer Welligent, LLC	(757) 668-6582	(757) 668-6575	mmccranie@welligent.com

System Issues

Name	Phone Number	Fax Number	E-Mail Address
Help Desk: Aprielle Barclift Welligent, LLC	(757) 668-6586	(757) 668-6575	abarclif@welligent.com
Technical Assistance: Charles Sutelan CEO Welligent, LLC	(757) 668-6428	(757) 668-6575	csutelan@welligent.com

Revised **02/03/04**

Points of Contact—LEADTRAX

Security Issues

Name	Phone Number	Fax Number	E-Mail Address
Nancy K. VanVoorhis LeadTrax Database Project Manager DCAH, VDH	(804) 864-7694	(804) 864-7723	nancy.vanvoorhis@vdh.virginia.gov
Joanne Boise Director DCAH, VDH	(804) 864-7685	(804) 864-7722	joanne.boise@virginia.gov
Michelle McCranie Security Officer Welligent, LLC	(757) 668-6582	(757) 668-6575	mmccranie@welligent.com

System Issues

Name	Phone Number	Fax Number	E-Mail Address
Technical Assistance: Rick Hasson, Programmer and Security Officer, Welligent, LLC	(757) 668-6450	(757) 668-6575	rhasson@welligent.com
Technical Assistance: Charles Sutelan CEO Welligent, LLC	(757) 668-6428	(757) 668-6575	csutelan@welligent.com

Revised **02/03/04**

VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment
www.vdh.state.va.us

Fax

To:	From:
Fax:	Pages:
Phone:	Date:
Re:	CC:

□ Urgent □ For Review □ Please Comment □ Please Reply □ Please Recycle

This facsimile transmission contains confidential or legally privileged information that is intended only for the use of the individual or individuals named on the transmission sheet. If you are not the intended recipient, you are notified hereby that any disclosure, copying distribution, or the taking of any action in reliance on the contents of this facsimile transmission is strictly prohibited. If you have received this communication in error, please call me collect immediately so that I can arrange for the return of the documents to me at no cost to you.